Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of	)	
	)	
Communications Assistance for	)	ET Docket No. 04-295
Law Enforcement Act and	)	
Broadband Access and Services	)	RM-10865

Comments of Verint Systems Inc.

Todd P. McDermott
Vice President – Business Development
Verint Systems Inc.
14900 Conference Center Drive
Suite 100
Chantilly, VA 20151

Filed: 20 December 2004

Table of Contents

EXECUTIVE SUMMARY

Verint Systems Inc. (NASDAQ: VRNT) is a leading provider of analytic software-based solutions for communications interception, digital video security and surveillance, and enterprise business intelligence. Verint provides digital recording and monitoring systems with multiple applications for law enforcement agencies, public network providers, contact centres, government and intelligence agencies. The company's products are installed in law enforcement agencies, telecommunication networks, financial institutions and other contact centres worldwide. Verint software, which is used by over 1,000 organizations in over 50 countries worldwide, generates actionable intelligence through the collection, retention and analysis of voice, fax, video, email, Internet and data transmissions from multiple communications networks.

Verint Systems Inc. has been developing and deploying CALEA compliant systems for over 5 years in the US market as well as providing similar technical solutions for numerous markets around the world. With this level of experience, Verint has prepared the following comments to the FCC NPRM dealing with CALEA and Broadband Access and Services. Furthermore, Verint is submitting these remarks after reviewing the initial public comment filings put forward to the Commission on this matter.

The following submission presents comments on certain items of the NPRM. The numbering scheme corresponds to the numbers of the sections published in the initial NPRM.

A. INTRODUCTION

No comments provided by Verint.

B. APPLICABILITY OF CALEA TO BROADBAND INTERNET ACCESS AND VOIP SERVICES

> 37. In this section, we tentatively conclude that facilities-based providers of any type of broadband Internet access service, whether provided on a wholesale or retail basis, are subject to CALEA because they provide a replacement for a substantial portion of the local telephone exchange service used for dial-up Internet access service and treating such providers as telecommunications carriers for purposes of CALEA is in the public interest. Broadband Internet access providers include, but are not limited to, wireline, cable modem, satellite, wireless, and broadband access via powerline companies. We seek comment on this tentative conclusion. In addition, we tentatively conclude that providers of VoIP services that Law Enforcement characterizes as "managed" or "mediated" are subject to CALEA as telecommunications carriers under the Substantial Replacement Provision. Law Enforcement describes managed or mediated VoIP services as those services that offer voice communications calling capability whereby the VoIP provider acts as a mediator to manage the communication between its end points and to provide call set up, connection, termination, and party identification features, often generating or modifying dialing, signaling, switching, addressing or routing functions for the user. Law Enforcement distinguishes managed communications from "non-managed" or "peer-to-peer" communications, which involve disintermediated communications that are set up and managed by the end user via its customer premises equipment or personal computer. In these non-managed, or disintermediated, communications, the VoIP provider has minimal or no involvement in the flow of packets during the communication, serving instead primarily as a directory that provides users' Internet web addresses to facilitate peer-to-peer communications. We request comment on the appropriateness of this distinction between managed and non-managed VoIP communications for purposes of CALEA.

VERINT: *37. Verint recognizes the technical distinction between "managed" and "non-managed" VoIP communications for the purposes of CALEA. Notwithstanding, it is Verint's view that access to both types of VoIP communications can be accomplished for the purpose of lawful intercept. The final set of call related data messages will likely vary between the two but will likely vary amongst all VoIP carriers based upon network topology, signaling schemes and what is "reasonably available". Verint holds that, through the use of broadband access technologies and an engineered solution, lawful access to the subject's call data, in whole or in part, and call content is achievable in*

both service models. Verint has successfully deployed solutions facilitating lawful access and delivery in both managed and non-managed architectures.

1. Analysis of CALEA's Statutory Definitions

a. "Telecommunications Carriers" under CALEA

No comments provided by Verint.

(i) The Substantial Replacement Provision - Section 102(8)(B)(ii)

No comments provided by Verint.

(ii) Telecommunications Carriers, Generally

No comments provided by Verint.

b. Application of Substantial Replacement Provision to Broadband Internet Access and Other Packet-based Services

(i) Broadband Internet Access Services

No comments provided by Verint.

(ii) VoIP Services

56. We tentatively conclude that providers of managed VoIP services, which are offered to the general public as a means of communicating with any telephone subscriber, including parties reachable only through the PSTN, are subject to CALEA. We believe that such VoIP service providers satisfy each of the three prongs of the Substantial Replacement Provision with respect to their VoIP services. That is, they provide an electronic communication switching or transmission service that replaces a substantial portion of local exchange service for their customers in a manner functionally the same as POTS service; and the public interest factors we consider at a minimum - i.e., the effect on competition, the development and provision of new technologies and services, and public safety and national security - support subjecting these providers to CALEA. We believe there is an overriding public interest in maintaining Law Enforcement's ability to conduct wiretaps of on-going voice communications that are taking place over networks that are rapidly replacing the traditional circuit-switched network, yet providing consumers essentially the same calling capability that exists with legacy POTS service. We

understand that basic capabilities essential to Law Enforcement's surveillance efforts, such as access to call management information (e.g., call forwarding, conference call features such as party join and drop) and call set up information (e.g., real time speed dialing information, post-dial digit extraction information) may not be reasonably available to the broadband access provider. Consequently, subjecting only the broadband access provider to CALEA without including managed VoIP service providers could undermine Law Enforcement's surveillance efforts. We seek comment on this analysis.

VERINT: *56. Verint agrees with the statement that access to some of the call management information may not be reasonably available to broadband access providers. However, it is our experience that each carrier's network is different, affording access to different levels of information. Both broadband access providers and managed VoIP service providers could, potentially, have access to varying amounts of call related data. For example, in both cases, by forwarding call content to a mediation device, post cut through dialed digits can be extracted and a call data message can be sent with this information while still, if required by the type of court order, inhibiting the call content flow to the LEA. Nevertheless, we contend that declaring that all call management services cannot be captured for the purpose of lawful intercept is too great a generality. In our view, each carrier or service provider should be required to make reasonable efforts to afford as comprehensive solution as possible within the "reasonable" guidelines of cost for the solution.*

2. Identification of Future Services and Entities Subject to CALEA

No comments provided by Verint.

C. REQUIREMENTS AND SOLUTIONS

No comments provided by Verint.

1 Carrier obligations under section 103

> 68. We tentatively conclude that we should apply the same criteria - i.e. information may not be "reasonably" available if the information is only accessible by significantly modifying a network-to broadband access and VoIP providers. We seek comment on this tentative conclusion. We recognize that, when looking at end-to-end service architectures, it is not always readily apparent where call-identifying information is available. We seek comment on where content and various kinds of call-identifying information are available in the network and further whether the information is reasonably available to the carrier. We anticipate that some call-identifying information may be available from either a VoIP provider or a broadband access provider. In these instances, would the call-identifying information be reasonably available from one entity but not from the other? If the information is reasonably available from both carriers, we expect that both carriers would have a CALEA obligation with respect to that information and would work cooperatively with each other and with the LEA to provide the LEA with all required information. We seek comment on these issues.

VERINT: *68. Verint, as stated before, contends that the information that would be "reasonably available" will differ from carrier to carrier and service provider to service provider based upon various technical factors. However, in our view, a key factor in successfully making the information from all sources available to the LEAs is to have not only carrier's work cooperatively with the LEAs, but to impose a similar obligation upon manufacturers. Verint believes, with a cooperative working arrangement amongst the three entities a cost effective CALEA VoIP solution can be deployed to meet the LEAs primary needs.*

2. Compliance solutions based on use of a "trusted third party"

> 70. The trusted third party approach recognizes that, even if a carrier does not process certain call-identifying information, that information may be extracted from that carrier's network and delivered to a LEA. The trusted third party obtains the call content and call-identifying information in either of two ways. The trusted third party could rely on a mediation device to collect separated call content and call-identifying information from various points in the network and to deliver the appropriate information to a LEA. Alternatively, the trusted third party could rely on an external system to collect combined call content and call-identifying information and to deliver the appropriate information to a LEA. We describe both of these models in Appendix C. We believe that the availability of a trusted third party approach makes call-identifying information "reasonably" available to a telecommunications carrier under section 103(a)(2). We seek comment on this analysis.

VERINT: *70. Verint has successfully deployed VoIP lawful intercept solutions which incorporate the means to extract call identifying information from a carrier's network.*

Verint solutions have the ability to facilitate the access to call related information so that the carrier can present a standards compliant delivery message set. This solution architecture involves the use of a mediation device to take network signaling information and develop the call data messages. Either the carrier themselves or a trusted third party could deploy such a solution. However, based on Verint's experience, it is unclear to us what additional information could be obtained outside a carrier's network that would not be readily available within the network itself. It is unclear to us how the addition of a trusted third party could enhance what call information would be "reasonably available" for the purpose of lawful access.

> 72. We seek comment on the feasibility of using a trusted third party approach to extract the content and call-identifying information of a communication from packets. In particular, we seek comment on whether an external system would be an efficient method to extract information from packets. It seems that external systems might provide economies of scale for small carriers. What would be the approximate relative costs of internal versus external systems for packet extraction?

***VERINT**: 72. In all existing VoIP solutions deployed by Verint, content and call identifying information are extracted from communications packets. The most significant technological challenge, in Verint's experience, has been associated with accessing these packets, not with decoding or extracting the underlying information. Again, as stated before, the use of a mediation device combined with various access devices can facilitate the achievement of this technical solution. Verint agrees that a trusted third party model clearly could allow the parties involved to take advantage of economies of scale, especially small carriers or carriers having small VoIP infrastructures. This could be achieved through the shared use of the mediation device(s) and delivery systems. However, Verint believes that each carrier's specific business case will undoubtedly show if the relative costs of an internal system or one deployed by a trusted third party is most cost effective.*

> 74. Reliance on a trusted third party may shift the burden now shared by carriers and manufacturers in complying with CALEA. For example, would it be adequate to require network equipment to provide only packet content under the terms of J-STD-025-A, and to allow the manufacturers of that equipment to assume that any additional analysis of the content will be provided by an external system? TIA asks "May a particular [network equipment supplier] conclude that its customers can find

other CALEA solutions from other suppliers, and at that point withdraw from the CALEA process without liability? . Could a supplier be forced to reenter the CALEA market if the third-party suppliers it was counting on go out of business?" What impact would reliance on a trusted third party have on developing standards for CALEA compliance? What tools would a service bureau need to interface with various products from numerous vendors and would this responsibility be difficult to meet or too expensive? Are there incentives to keep manufacturers engaged in developing CALEA compliance solutions if carriers relied on a trusted third party?

VERINT: *74. As a manufacturer of lawful intercept solutions worldwide, Verint contends that the business case for each carrier regarding the choice of an internally deployed system or one deployed by a trusted third party will define the final decision made by each such party. Verint develops CALEA compliant solutions and has deployed many systems in North America. We have found, in our experience that each system has to be engineered to meet the differing needs, both operational and technical, of each customer. Verint contends that, even with the use of a trusted third party, this same effort will still be required. Finally, Verint contends that, in both cases, a cost effective solution can be created to meet the needs of the customer and we will continue to develop CALEA compliant solutions as technologies change and as the standards evolve.*

3. Compliance solutions based on CALEA "Safe Harbor" standards

79. Although pursuant to section 107(b) the Commission may, upon petition, establish rules, technical requirements or standards necessary for implementing section 103 "[i]f a Government agency or any other person believes that such requirements or standards are deficient," the Court has determined that were it to allow the Commission to mandate modification of an industry standard "without first identifying its deficiencies, [the Court] would weaken the major role Congress obviously expected industry to play in formulating CALEA standards." We ask parties to comment on industry standards for packet-mode technologies in an attempt to determine whether any of these standards are deficient and thus preclude carriers, manufacturers and others from relying on them as safe harbors in complying with section 103. By doing so, however, we do not intend to inhibit the ongoing work by standards organizations, carriers and manufacturers to develop and deploy CALEA-compliant facilities and services. We recognize that CALEA provides that carriers and others may rely on publicly available technical requirements or standards adopted by an industry association or standard-setting organization to meet the requirements of section 103, unless the Commission takes specific action in response to a petition.

VERINT: *79. Verint believes, as a vendor of both access/delivery systems and monitoring center systems, that there is a benefit in developing and adopting industry standards for the delivery interface for CALEA solutions. In some cases, such as the cable industry, there is also a benefit in defining the "d" interface. Nevertheless, Verint believes that both the LEAs and carriers would find benefit in having an industry standard for lawful intercept delivery. This would, in our view, ultimately, reduce the costs and reduce the inevitable challenges and/or controversy for both parties.*

> 80. As an initial matter, we invite comment as to whether there is any need to define what constitutes publicly available technical requirements or standards adopted by an industry association or standard-setting organization. It appears that any group or organization could publish a set of technical requirements or standards and claim it to be a "safe harbor." Should we interpret the above terms to mean only standards developed by organizations recognized by the American National Standards Institute ("ANSI")? Should these terms also cover technical specifications that are developed and published by other types of industry organizations, such as CableLabsr, which is a consortium of cable TV system operators? Should we also recognize standards developed by non-U.S. standards organizations, such as the European Telecommunications Standards Institute?

VERINT: *80. Verint contends that utilizing other standards bodies' work can aid in developing domestic standards for lawful intercept within the United States and North America. Standards bodies recognize that technological differences as well as legal distinctions between the US and other countries will require some customization of the standards. However, through the use of other standards bodies' work such as ETSI, we would expect domestic standards to be expedited and that this would also reduce the underlying costs associated with their development.*

> 83. For voice over packet (a technology used to provide most or all broadband telephony services), post-connection DDE is not required to be isolated and provided to LEAs under T1.678, T1.724, J-STD-025-B, or PKT-SP-ESP-I03-040113. A VoIP caller may also connect to an IXC, and the post-connection dialed digits may also identify the 'origin, direction, destination or termination' of the communications. We seek comment on whether DDE in packet networks is call-identifying information for the same reasons that we have previously concluded that it is in circuit-switched networks. Are there differences in packet technology that would preclude post-connection dialed digits from being termed call-identifying information? Are there differences in packet technology that would preclude post-connection DDE from being readily achievable? Is the omission of DDE or other punch list capabilities from these standards a deficiency under the terms of section 107(b)?

VERINT: *83. The Verint STAR-GATE system for VoIP includes, as an option, the ability for the user to decode post cut through dialed digits. In the case where DDE is required, the system is configured to deliver call content packets to a mediation device. Contained within this mediation device is the required hardware and software to enable the user to actively interpret post cut through dialed digits. The dialed digits are encoded into a call data message and delivered to the LEA. If required, the call content may be inhibited from delivery to the LEA or delivered, as configured by the user based upon the type of court order. Thus, based on our prior experience, in our view DDE is reasonably achievable.*

> 84. Second, when broadband telephony call-identifying information is provided to LEAs, Law Enforcement may have concerns with the format of the electronic interface used to provide this information as described in T1.724 and under one option in T1.678. The issue is whether the industry can send LEAs copies of messages used by voice over packet systems that use terminology specific to the technology or function, or whether the messages must be converted into a format and common language more consistent with the messages in J-STD-025 and PKT-SP-ESP-I03-040113. The kind of format used in J-STD-025 and PKT-SP-ESP-I03-040113 is preferred by Law Enforcement. We seek comment on what difficulties LEAs may encounter if information is provided in different formats, depending on the underlying transmission source. We also seek comment on whether uniformity of formatting is needed to satisfy the requirements of section 103(a)(3) concerning delivery of intercepted communications and call-identifying information.

VERINT: *84. Verint contends that the use of an industry recognized standard for lawful intercept information delivery should preclude LEAs from encountering problems in collection or decoding/demodulating. However, Verint recognizes that certain delivery standards do not compel the use of a specific vocoder format, thus significantly complicating LEA playback in many cases. Verint suggests that the standards groups address this issue by publishing a restricted list of industry standard vocoders for the use in transmission of packet mode call content to the LEA. Verint understands that this may require additional development of transcoding capabilities within the lawful intercept delivery systems. However, the engineering costs to facilitate this in a carrier's solution should be minimal in scope versus the unbounded requirement currently levied on the monitoring center manufacturers.*

4. CALEA compliance for satellite networks based on system-by-system agreements

> 86. Next, we tentatively conclude that continued use of system-by-system arrangements is the appropriate method for satellite systems and will aid in meeting the goals of CALEA. We note that satellite carriers have used an approach based on negotiation, resulting in private agreements to provide information to LEAs. Satellite networks differ in fundamental ways not only from terrestrial networks but also from each other. These differences arise from unique aspects of the type of satellite used in the network (e.g., non-geostationary vs. geostationary satellites) and the gateway earth stations that may be located both within and outside the United States. System-by-system agreements between LEAs and satellite carriers account for the unique aspects of each system. For example, the agreement between Iridium Constellation LLC ("Iridium"), DoJ, and the FBI requires that Iridium pass all domestic communications (defined as (i) wire or electronic communications that originate and terminate within the U.S. and (ii) the U.S. portion of a wire/electronic communication that originates or terminates within the U.S.) through "a facility under the control of Iridium and physically located in the U.S., from which Electronic Surveillance may be conducted." Similarly, the LEA agreement with Telenor Satellite, Inc. requires that all domestic communications be transmitted through U.S. earth stations or routed through a point of presence "that includes a network switch or router under the control of" Telenor that is located in the U.S. We tentatively conclude that continued use of system-by-system arrangements is the appropriate method for satellite systems and will aid in meeting CALEA's goals. We seek comment on this tentative conclusion

VERINT: *86. Verint has deployed lawful intercept systems in satellite networks and, as a result of this experience, agrees with the Commission's conclusion that a system-by-system solution is the most appropriate way to address this specific type of carrier. However, as stated before, Verint sees the benefit of utilizing a standards based delivery interface along with a restricted list of call content vocoder formats.*

D. CALEA COMPLIANCE EXTENSION PETITIONS

1. Background

> No comments provided by Verint.

2. Discussion

> 91. We support Law Enforcement's goal of strengthening the CALEA implementation process. We agree that timely implementation of both circuit-mode and packet-mode technology by telecommunications carriers is essential to ensure

that electronic surveillance can be readily and efficiently performed. However, we believe that Law Enforcement's goal can be achieved without us imposing the implementation deadlines and benchmark filings it requests. We recognize that carriers have continued to rely on CALEA section 107(c) when submitting extension requests for packet-mode compliance. We intend to resolve the status of those petitions in this proceeding, but in a way that is not unduly disruptive. Accordingly, we intend to afford all carriers a reasonable period of time in which to comply with, or seek relief from, any determinations that we eventually adopt. We tentatively conclude that a "reasonable period of time" is 90 days and request comment on this tentative conclusion. We may, on less than 90 days notice, require any or all carriers to provide additional information to support their extension requests. We seek comment on all issues identified in the following analysis, as well as any other issues that relate to disposition of pending and future extension requests.

VERINT *91. Independent of the final outcome associated with these particular issues, Verint wishes to re-affirm the fact that we have deployed network-wide, comprehensive VoIP lawful intercept solutions in various countries around the world. Thus, Verint contends that extension requests based upon the unavailability of a technical solution should not be considered. We understand that each carrier's solution will, most likely, be somewhat unique and require time to engineer, install and commission. However, in our view, each solution can be crafted from existing commercially available elements, customized in configuration to meet the carriers' respective needs.*

a. Disposition of Circuit-Mode Extension Petitions

No comments provided by Verint.

b. Disposition of Packet-Mode Extension Petitions

(i) Background

No comments provided by Verint.

(ii) Availability of Sections 107(c) and 109(b) in Connection with Packet-Mode

98. Moreover, we believe that carriers face a high burden in making an adequate showing to obtain alternative relief pursuant to section 109(b). Under the requirements of that section, carriers must demonstrate that compliance is not reasonably achievable, and we must evaluate submitted petitions under the criteria set out in section 109(b)(1), including cost and cost-related criteria and an assessment of

the effect of any granted extension "on public safety and national security." It would be difficult for a petitioner to make such a showing unless the request was made in connection with precisely identified "equipment, facilities, or services." As explained more fully below, under the requirements of section 109(b)(1)(B) and 109(b)(1)(D), such a demonstration would need to include a thorough analysis of precisely identified costs of upgrading the carrier's network to satisfy CALEA obligations and of other difficulties, as well as their effects on ratepayers; general allegations that projected costs were "too high" or unreasonably burdensome would not suffice. We tentatively conclude that the requirements of section 109(b) would not be met by a petitioning carrier that merely asserted that CALEA standards had not been developed, or that solutions were not readily available from manufacturers. Unlike section 107(c), section 109(b) contains no requirement that we evaluate what is "reasonably achievable" with reference to available technology. We recognize, however, that carriers may bring to the Commission's attention section 107(c) requirements in the context of a section 109 petition, under the heading "such other factors as the Commission determines are appropriate." If standards or solutions do not exist, petitioning carriers would still need to demonstrate why they could not negotiate system-specific CALEA solutions with manufacturers or with third-party CALEA service providers. In short, we believe that petitioners that purchased and installed non-CALEA compliant equipment after the CALEA compliance date bear a heavy burden to show why they could not have selected CALEA-compliant equipment. That showing must include a demonstration that the petitioning carrier exercised due diligence to obtain CALEA-compliant solutions from manufacturers or third-party service providers. We seek comment on this analysis.

VERINT: *98. In the absence of a generally accepted or imposed standard, Verint has deployed lawful intercept solutions and provided its customers and LEAs details about the interface, along with sample data designed to facilitate operational success. It should be noted, that inherent in the STAR-GATE product design is the ability to easily configure to migrate to a standards based solution once a standard has been adopted. The carrier thus has the means to move to a standards based solution cost effectively.*

(iii) Section 109(b) Petition Requirements

No comments provided by Verint.

c. The Alternative Extension Mechanism Proposed by Law Enforcement

No comments provided by Verint.

E. ENFORCEMENT OF CALEA

No comments provided by Verint.

F. COST AND COST RECOVERY ISSUES

No comments provided by Verint.

1. Cost Recovery for Post-January 1, 1995 CALEA Compliance

No comments provided by Verint.

2. Intercept Provisioning Costs

No comments provided by Verint.

3. Jurisdictional Separations Implications

No comments provided by Verint.

G. EFFECTIVE DATE OF NEW RULES

143. If the Commission ultimately decides that entities that heretofore have not been subject to CALEA will have to comply with its requirements, we seek comment on what would be a reasonable amount of time for those entities to come into compliance with sections 103 and 105 of CALEA. Should newly-identified entities either come into compliance with or seek relief from section 103 requirements within 90 days, as we propose for carriers that have filed section 107(c) petitions? Or should newly-identified entities have 15 months to come into compliance with section 103, as Law Enforcement suggests, or is some other amount of time reasonable? Regarding compliance with CALEA section 105 and section 229(b) of the Communications Act, should newly-identified carriers comply with the system security requirements previously adopted by the Commission within 90 days, which was the amount of time the Commission provided when it adopted those rules, or is some other amount of time reasonable? Commenters should address factors that would support their suggestions for sections 103, 105 and 229(b) compliance deadlines.

VERINT: *143. As indicated in previous sections, Verint has deployed lawful intercept solutions for VoIP networks. Thus the contention that manufacturers have not developed solutions is, in Verint's view, somewhat unfounded and misleading. In regard to the time period provided to carriers to come into compliance, Verint feels that a period of 12 months is quite reasonable and achievable. Especially in light of the fact that this proposed period does include allowances for engineering the solution and contract administration activities.*